

Documentation for the swtor add-on for tails V 0.52

Authors : swtor00@protonmail.com
Date : 01.04.2021
License : GPL 2.0
+

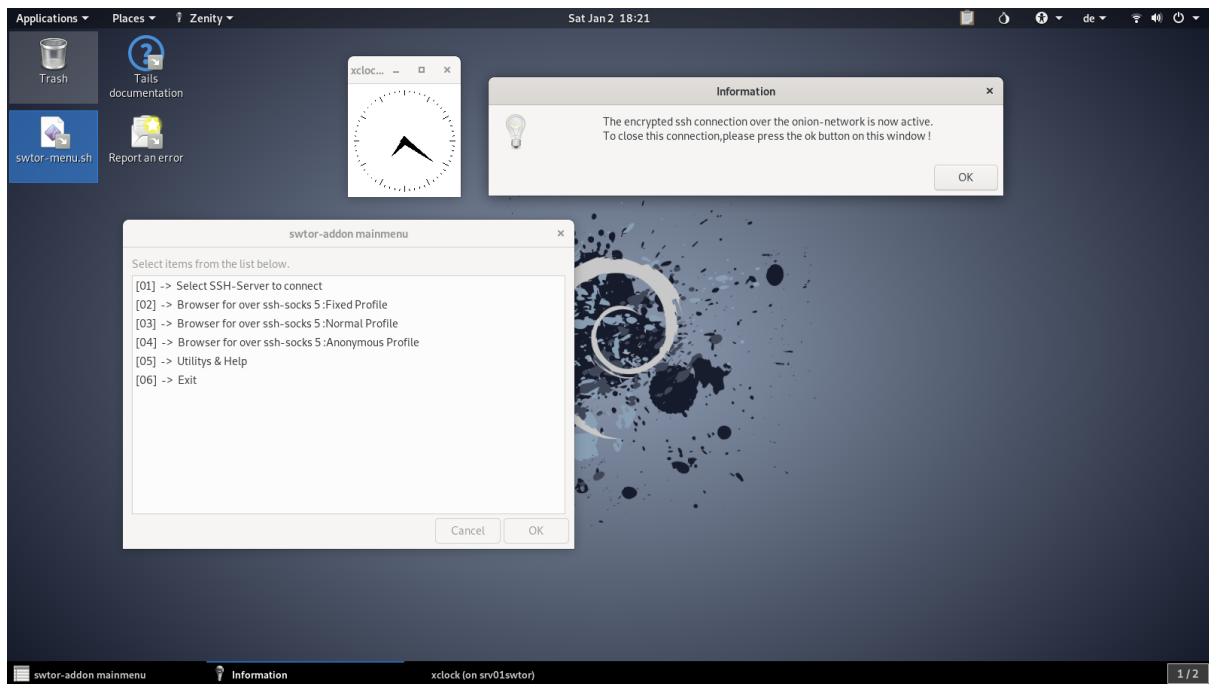


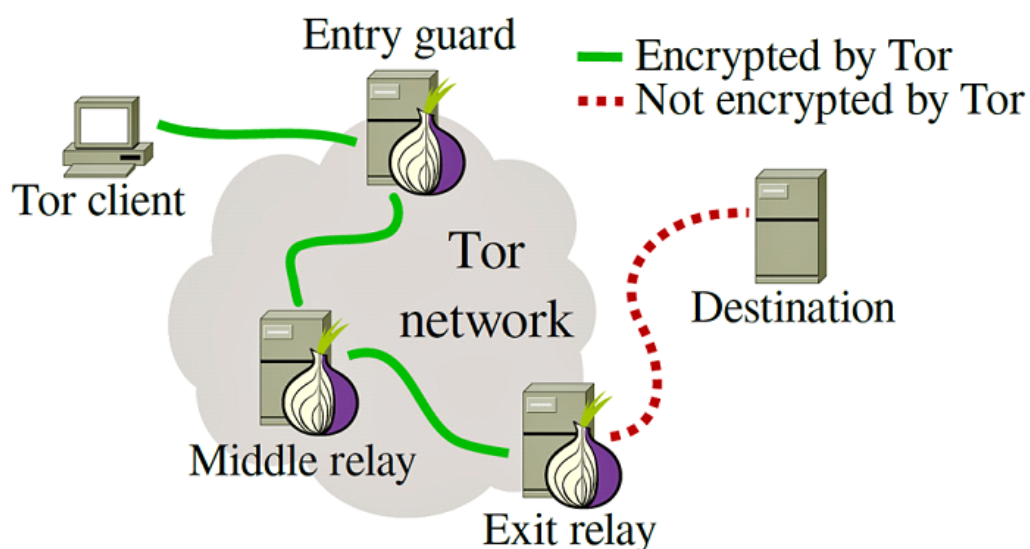
Table of contents

Title page	1
Table of contents	2
Introduction	3
1.0 Using your own SSH server inside your own Network at home	13
2.0 Using your own SSH-server external	15
3.0 Using a remote SSH-server anywhere on the Internet (Best scenario)	18
4.0 Preparations prior to use of this add-on	22
5.0 Installing the add-on	25
6.0 Configuring the required SSH-connection for the add-on	30
7.0 Executing the add-on for the first time	36
8.0 Use of the add-on, after the first initial run	34

Introduction

This documentation describes how to install and use this add-on for Tails-Linux Version 4.14 or later. You may ask yourself, why do I need such a add-on for Tails ? The Tails Linux system already protects your privacy by using the Onion-Network on every startup. It is also true that a Tails system already makes a very good job to hide your true identity and real IP-Address to the websites you are visiting.

Although, it seems many Tor users are having difficulties surfing and navigating the regular World Wide Web (sometimes called Clearnet Internet) , as some websites have set up discriminating rules against people who are using the Tor Browser to browse the web. At any specific moment in time when we are using Tails or the TOR-Browser in general, our personal IP packets are sent through the Internet crossing 3 different Nodes to hide the origin where the packets came from.



The last of this 3 nodes so called “Exit-Nodes” or “Exit-Relay” of the Onion-Network can easily and instantly be detected as soon as someone queries with any remote IP Address from the list below.

<https://check.torproject.org/cgi-bin/TorBulkExitList.py?ip=1.1.1.1>

Therefore it is no longer a secret to any website, that we are using the TOR-Browser or even Tails and they will often run this act of “captcha terror” against regular users of the TOR-Browser.



or something similar like this beloved one ...

Jane

Last Name

Smith

Email

stopall

Pick your color


☒ Red




☐ Green

☐

Submit

Select all squares with street signs.

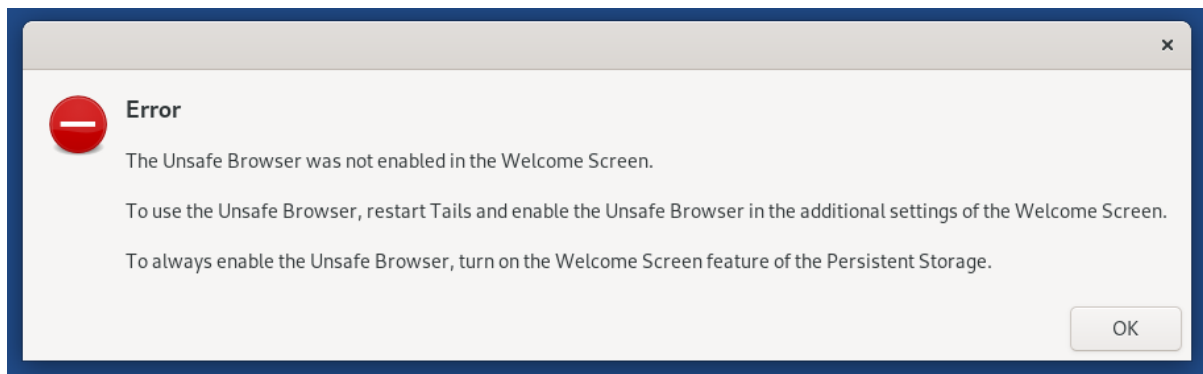




VERIFY

Alarminglly, the number of websites that completely block or run the “captcha terror” against regular TOR-Users is growing in numbers day by day, to the detriment of Tor’s usefulness.

Integrated inside of every Tails installation on a CD or USB medium, there is still the so called “Unsafe Browser”. Because this “Unsafe Browser” doesn’t make any use of the Onion-Network at all, all data communications from this browser can easily be logged by your Internet Service Provider (ISP) or your government. After Tails Version 4.14 was released, it was possible to completely prevent the starting of the unsafe Browser inside of Tails.



By the default settings from greeting screen of tails 4.14 or higher, the start of the “unsafe Browser” is not longer possible until a user set the default value from “not starting “ to “allow starting”.

It may make sense to use the “Unsafe Browser” inside Tails solely to browse a captive portal like it is used in many public WiFi networks, but not really for more than this simple task.

https://tails.boum.org/contribute/design/Unsafe_Browser/

Prior to activate the use of the unsafe Browser in the greeting-screen , please keep the following in mind.

IF YOU DON'T NEED THE UNSAFE BROWSER ...
DON'T ACTIVATE IT AND USE IT !!!!

Some smart people even try to start a VPN connection with OpenVPN or something similar to hide the fact that they are using the Onion-Network, which can be blocked by any website or even an ISP.

Apart from the fact that you are only able to use a single TCP port for the very popular OpenVPN communication (all possible UDP ports inside of Tails are blocked by default), it produces many more problems than it would solve. In the endless debate about the use of a Virtual Private Network inside of Tails, I recommend to read the following URL.

https://tails.boum.org/blueprint/vpn_support/

“Similarly, we don't want to support VPN's as a replacement for Tor since that provides terrible anonymity and hence isn't compatible with Tails' goal.”

What we want

Tails -> Tor -> VPN

USE CASES

1. Access services that block Tor.
2. Reach a local resource on a VPN that is not accessible in any other way.
3. Reach a VPN non-anonymously (e.g. your account is tied to you URL) while only hiding your geo-location, which may be the only thing you need in some situations. (Maybe invalid since this is not part of the PELD spec (yet?) AFAIK.)

SOLUTION

The easiest solution for this case 1 (which we feel is the most important one for this Tor/VPN setup) is to use an SSH connection with the Dynamic Forward option. The newly created SOCKS port can be used to have a fixed outgoing IP address. We may document how to use this in an "unsupported, advanced users only, “may kill kittens” part of the documentation.

Now, exactly right here, my special add-on for Tails enters the game called “Privacy,” and provides some very useful functions for the many Tails users out there :

- Use of an encrypted SSH-connection to a Remote Host and building of a local socks5 proxy. Even the traffic that is sent over the so called “Exit-node” of our communication is still encrypted until it reaches the destination SSH-Server. When the connection packets leave the SSH-Server to any external website as a example, the packets are not longer protected by SSH and would look like a ordinary traffic from a Desktop Computer running Linux.
- All SSH traffic is encrypted and routed over the Onion-Network, as long you are using an SSH server anywhere on the Internet. If you are using a SSH Server at your own network at home, only the internal connection from you tails system to the other internal ssh server is encrypted. And I guess only, this is not the way you would like to go to hide the fact that you are using tails ...
- A local Browser (Chromium) with three different profiles that can be used to visit TOR unfriendly websites like Google, and many other websites that would block regular TOR users like second class Internet users. All three predefined Chromium profiles are protected against multiple actions like WebRTC and trackers in general.
- All local DNS resolution traffic on UDP Port 53 is routed over the local socks5 proxy to the remote SSH Server . This means you never contact you local used DNS Server (router or DNS from your ISP)in any way, like you would do with the unsafe browser.
- For any particular website, anywhere on the Internet, it is no longer possible to detect that we are using the so called “Onion Network” to hide our personal information or IP address at all. All the traffic that the owner of the website can analyze, is coming from the regular public IP address of the remote SSH server we are currently connected to. The fact that we are using the “Evil Onion-Network” to establish our SSH connection, is not visible to the websites we are visiting.

One huge problem still remains with using the Tails system to contact onion-unfriendly systems. It makes no difference what kind of bypass protocol is used to hide the fact that we are using Tails or the onion-network in the background. This so called bypass systems could be done by one of the three following techniques.

- A remote SSH-Server using a local socks5 connection port. This is the connection type we are using inside of the add-on and is the recommend way of the developers of tails.
- OpenVPN Server with a single TCP connection.
- Proxychains

All other currently wildly used Virtual Private Network solutions (LL2TP / IPSEC as a example) that would rely on a active UDP connection, would not work inside Tails because UDP protocol isn't supported at all.

By now follows a little Warning about using any of the bypass systems inside of tails including this add-on itself !

At this point you would like to raise awareness about the trust you are willing to give to a foreign host system and his administrators and users as well, who could easily read your complete communication that would be sent through to the foreign server you haven chosen to connect.

If you would like to use any of the 3 above bypass techniques, please don't underestimate the control they have over you in the exact moment in time that you are using their servers to connecting to a remote Websites. Almost any VPN Service provider worldwide out there on the Internet make claims on their websites with cheap marketing statements like the following ones:

“We don't log anything !”

“We don't spy our users !

“We protect the privacy of our customers !”

Some very interesting articles about the “no-log policy” of some very popular

VPN providers can be found here.

http://www.theregister.co.uk/2011/09/26/hidemyass_lulzsec_controversy/

<https://torrentfreak.com/ipvanish-no-logging-vpn-led-homeland-security-to-comcast-user-180505/>

<https://www.techworm.net/2018/08/reasons-why-shouldnt-use-free-vpns.html>

<https://www.techrepublic.com/article/16-popular-vpns-leak-your-data-heres-the-full-list/>

If you read the above articles carefully, you may come to the final conclusion that you shouldn't give your personal trust out to the first person or company who offers you a VPN or SSH account for free. Even if you pay for a service with a monthly fee, there is really no guarantee that you aren't being "tracked" by this VPN server or any other active users of the remote system.

Prior to show 3 possible working scenarios with my add-on, we have to talk about the dangers using it at all. From all next described scenarios, you only should use the last presented scenario if possible.

- Never do a login with a username or email-address that you ever used on the normal Internet anytime. This kind of internet connections could be easily tracked back to you as a person or a company. This includes of course any kind of login for email, twitter or Facebook. If you need access to any website with your real email while you are using tails, use better a other computer of your home network or do a reboot to using Windows or Linux.
- Only use my script to solve problems with tor-unfriendly sites at all and if ever possible try to use the more secure builtin tor browser of tails to connecting it.

- Never using any website simultaneously inside of the TOR-Browser and the Chromium Browser used by the script.
- Don't use your mobile phone for a 2-Step verification while you are using Tails or the TOR-Browser.
- Don't operate on a user account created for Tails only, outside of Tails in any way. This also means you never send any email from your public Email Address to a Email Address you created for Tails only. And you never send a personal Email from a Tails only address, to someone else you ever contacted outside of tails.
- Don't post any personal information that can be tracked back to you.
 - Emails-Addresses that you ever used outside of tails
 - Never use a nickname inside of tails, that you ever used in the past history on the internet
 - Credit card Information
 - Phone Numbers
- Don't use Google for searching, even if you are connected to a remote server over SSH, that could use the Google Search Engine. Better use the following alternatives :

www.startpage.com

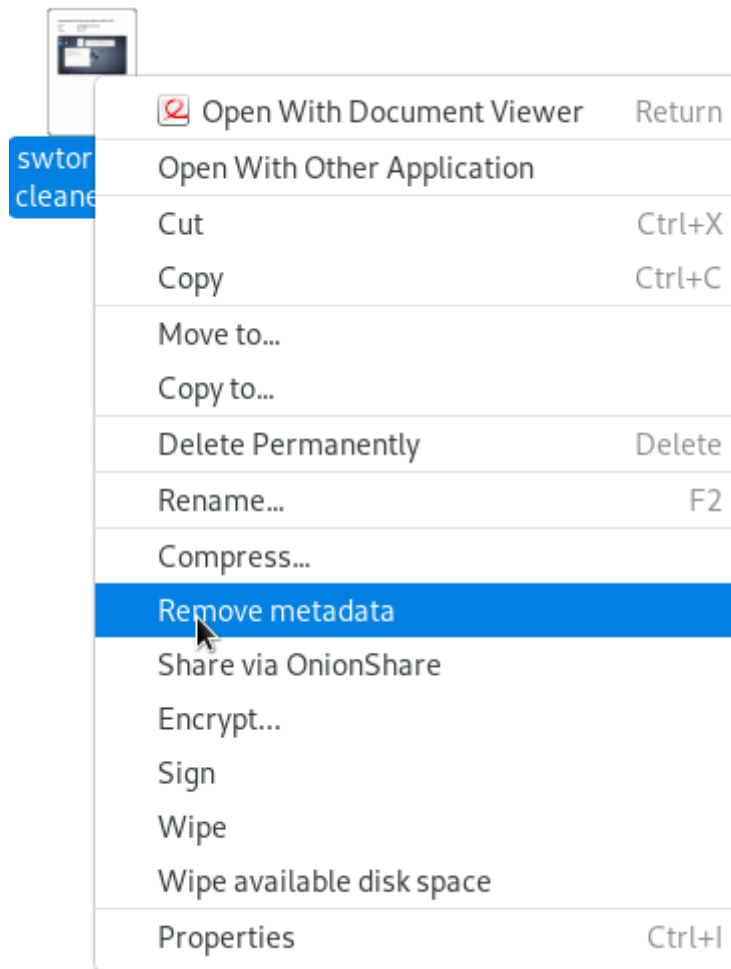
or

www.duckduckgo.com

- Never post any data like photos or documents without any uncleaned meta data inside. Inside of tails it is possible , to clean up all meta-data with a single click over the file-manager.

https://tails.boum.org/doc/sensitive_documents/metadata/index.en.html

On the following screenshot, you see how easy it is to remove all meta-data from a existing file.



To be honest, it would be very stupid to follow exactly all the above guidelines to be invisible on the Onion-Network and with a single published photo taken from your Smartphone, you may publish Data like the following ones over the Meta-Data field.

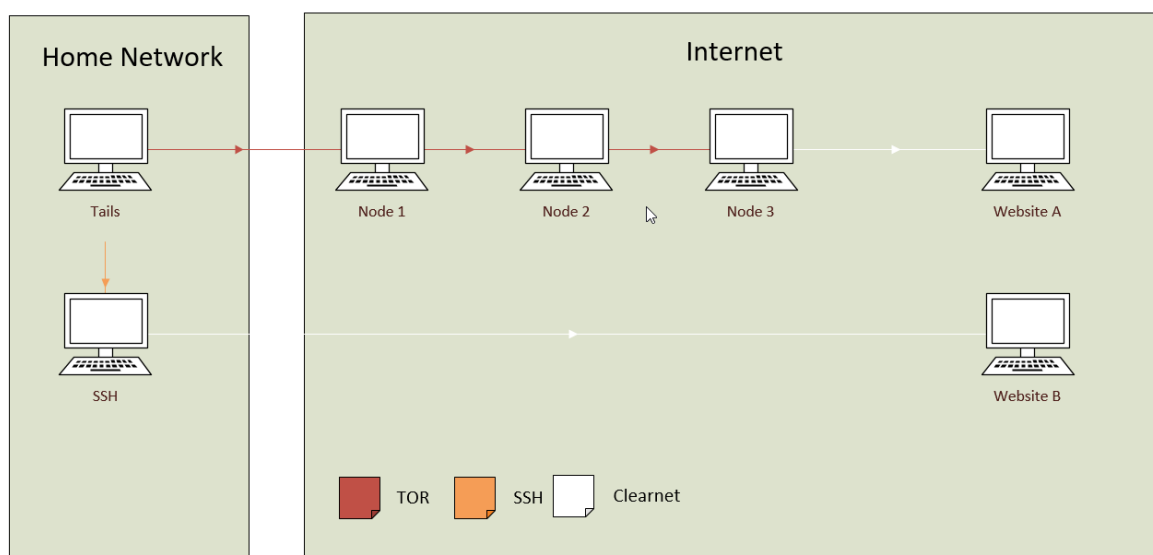
- Send the exact location where the photo was made.
- IMEI or Serial number of your used smartphone.

1.0 Using your own SSH Server inside you own Network at home

For this simple and not really recommend scenario, you need at minimum, a second computer with Linux or Unix running on your own network at home. For this SSH-daemon you could use, for example, a simple Raspberry-Pi, or of course, any other computer with an SSH daemon would work as well. This could be implemented with a Linux System like Debian or many others without any problem. For a simple example to build a SSH-server on a Raspberry-Pi I would recommend the following URL.

<https://www.raspberrypi.org/documentation/remote-access/ssh/>

Scenario 01:



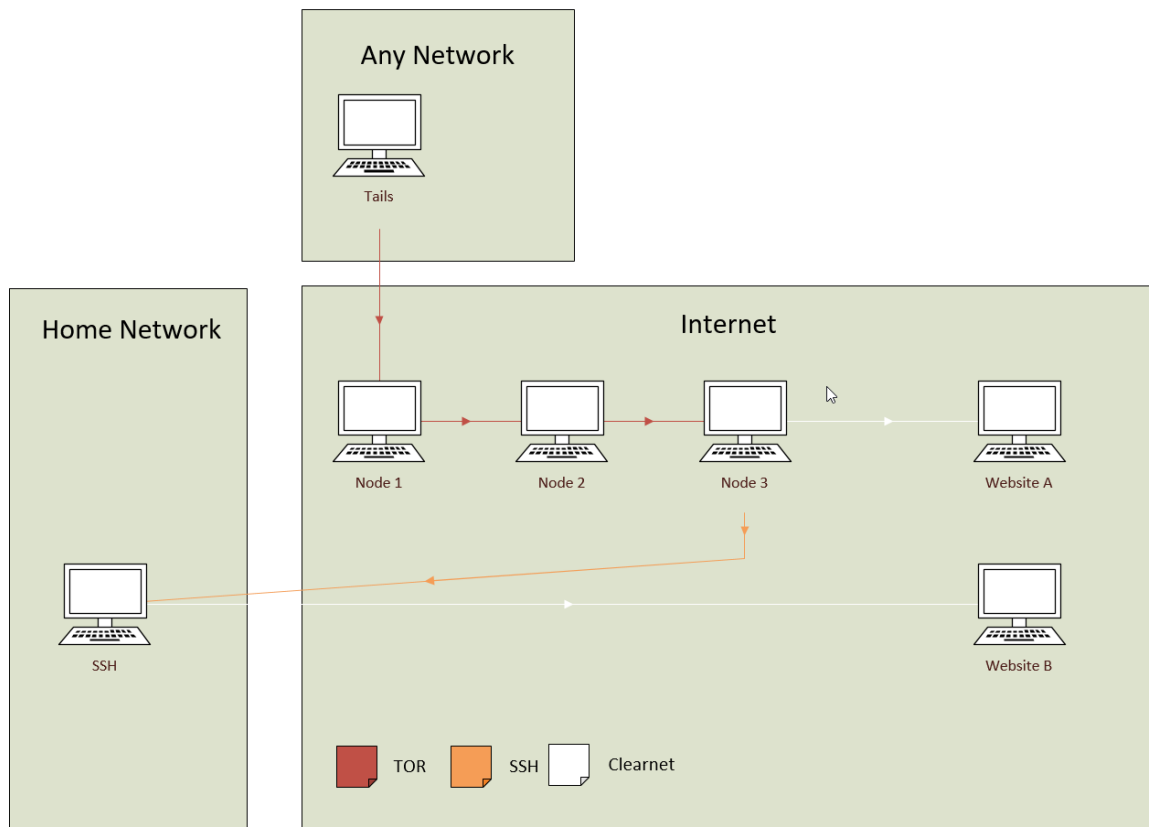
If you are using this “not so perfect scenario”, you can do the following:

- Use a Website like Google or many others that normally would block your connection. To be reminded again ! The complete Internet traffic (Data) that you send via my script through the Internet (from the SSH-server at your home to Website B for example), can be tracked and analyzed by your ISP, because it would be coming from a regular computer inside your home network !

- Only the websites that you are visiting with the TOR Browser over the Onion-network are secure to visit without to being tracked (Website A for example). Of course, you could also use the “Unsafe Browser” of tails to visit any website you wish, as long the *Unsafe Browser” is enabled on startup of tails.

2.0 Using your own SSH-server external

Scenario 02



If you would like to connect to the home ssh server externally from the Internet with Tails, there is some additional work to do.

- Port Forwarding of TCP port 22 (or any other desired port you would like to use) to the destination IP inside the home network needs to be enabled. This has to be done inside your router or firewall, depending what device you are using to connect to the Internet. Most users own a router for connecting to the Internet.
- Do not allow Root Logins over SSH (PermitRootLogin no)
- Allow only a single user to login over SSH (AllowUsers username)

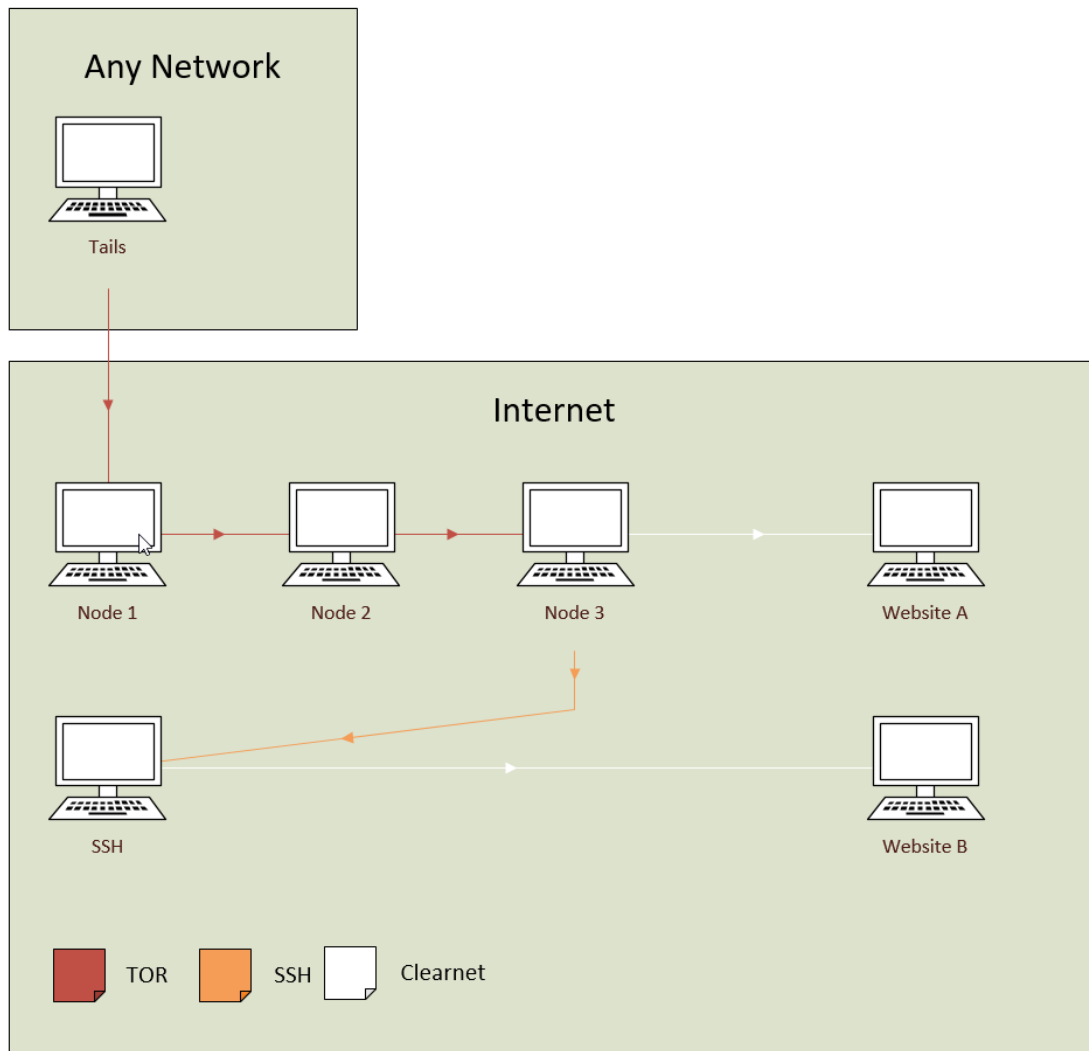
- Enable a DYNDNS name for your WAN IP, because most ISP's don't provide fixed IP-Addresses for the customers WAN interface. If you need a DYDNS name for your connections to the home network, I would call it a security hole that your often not aware of.
- As soon this system is reachable from the Internet, special considerations need to be applied for the security of our SSH daemon at home.
 - You may not use the standard TCP port 22. A very good replacement port would be TCP port 443 or 53.
 - Use a key instead of a password.
 - Disable all password logins after successful logins with a key.
 - Put the SSH-daemon on a schedule,if you know you'll want it before hand.
 - Fake the login message to mislead the snoopers or any disliked persons.
 - Only use SSH-V2, The older protocol V1 shouldn't be used anymore.
 - Disable empty passwords for all accounts.
 - Always update your system to the latest versions available because your computer could be contacted directly from the Internet.
 - Your computer at home needs to be up and running all the time if you want to contact the your home server from any location over the Internet.

I would like to emphasize the importance of the fact, like in the previous scenario, all traffic that you send over the remote SSH-Server can be traced by your home ISP or a local government. If you are placing the SSH-server like this in a company environment, the staff of the involved company could also tracking all your traffic.

In this particular case it may even better to use the “Unsafe Browser” of Tails, of course it could also be tracked by the local ISP that your are currently connected to, but not by your home ISP if you are using the local “unsafe Browser” of Tails.

3.0 Using a remote SSH-server anywhere on the Internet (Best scenario)

Scenario 03 :



As you may now see, there are so many things that have to be configured correctly with SSH, especially if your own SSH-server can be reached from the Internet. If you don't have a second computer inside your own network, the only suitable solution would be to find an SSH-provider anywhere on the Internet. This third option is the best option for all possible solutions to build your SSH-connection externally from Tails.

The difference from this Scenario compared to the two previous presented scenarios, is that your currently used ISP can only see the TOR traffic to the Internet. To be a bit more precise, your current ISP can only track the connection made to the first Node (Node 1) of the chain. Every TCP packet you send to through the Internet passes through 3 different nodes until it reaches the desired destination.

During this even the complete communication between the Node 3 (Exit-Node) and the foreign SSH server is encrypted until your packets have left the SSH-server. With all the above described scenarios , one thing should highly emphasized.

You can't hide the fact, from your currently connected ISP, that you are using the TOR-Browser or even Tails. If you really want to hide the fact that you are using TOR or Tails, you have to do that at your own risk and against the wise advice from the creators of Tails.

https://tails.boum.org/doc/first_steps/startup_options/bridge_mode/index.en.htm

So where should you start looking for a public SSH-server on the Internet ? As a good recommendation and starting point, you should have a look at the following URL :

<https://shells.red-pill.eu/>

Once again, we emphasize that you should only visit these multiple freeshell websites in the above link with the Tor-browser or Tails. If you are visiting them with a clearnet browser on linux or windows, you may have done a step too much to hide your personal information.

Another piece of advice from me is to use a fake-email address to register for a SSH-service of your choice. I'm sure you will find many SSH-providers on that ssh serverlist that meet some or all of your current requirements for a good SSH-provider. And as a third and last piece of important advice from me, never create a username for a login that could be traced back to you.

- Some of them are free of charge, others are not. If you ever pay for service, please use attention to use only a prepaid credit card that can not tracked back to you !
- The process to create a valid account depends from server to server.
 - The only thing needed to create a account is a e-mail account.
 - A Email and a written postcard.
 - A little riddle to prove your knowledge about Linux and Unix in general
- Some of them don't ask for personal information about you, others would like to know almost everything about you.
- Not so many providers from that daily growing list, give a full shell-account including a new email address or the option for X11 forwarding.
- Many of them provide a little space to host a website on the server .
- A few of them have databases like mMariadb or MySQL.
- The provided disk space to store personal files is very often limited to between 20 MB or even less.
- Some of these listed SSH-servers would work very well, as long you aren't trying to connect to them over the onion network. At the same moment you try to login over a public exit node from the onion network to that SSH-server, they terminate the connection immediately. Like the so many tor unfriendly websites we are already talked about, this servers are ware aware of, that we are connecting over the ONION-network. They block us ...

But wait, Yes ... there is a nice clever solution for this little handicap. At first we make a first SSH-connection to a external server that allows us to connect over onion-network. From our first connected SSH "Jumpserver" we make the desired connection to our second SSH-server. This setup is definitely not easy to configure, but it will work.

Almost all shell-providers of this provided red-pill list do not allow the following “bad things”.

- Only allows 1 active Connection with one registered login. Multiple connections with the same login would be detected instantly and the user would be banned.
- Many of the SSH-Servers on that list can not be reached over the Onion-network directly. There is exactly one Server on the list, that I know of, it is possible to connect over the Onion-Network. To be honest, I use this server very often as well.
- Not allowed to “share” accounts with friends or other persons.
- The installation of your own software or malware files is strictly forbidden.
- The use of port scanners like nmap against other servers on the Internet.
- The use of software like “P2P” or “Torrent-clients” is strictly forbidden.
- On some servers is IRC allowed, on others completely forbidden.
- Some of these listed systems have hundreds of active users so be nice and keep in mind that there are other users as well and don’t use up all the resources of a remote server. (Like CPU, Memory, Disk space or even Bandwidth)

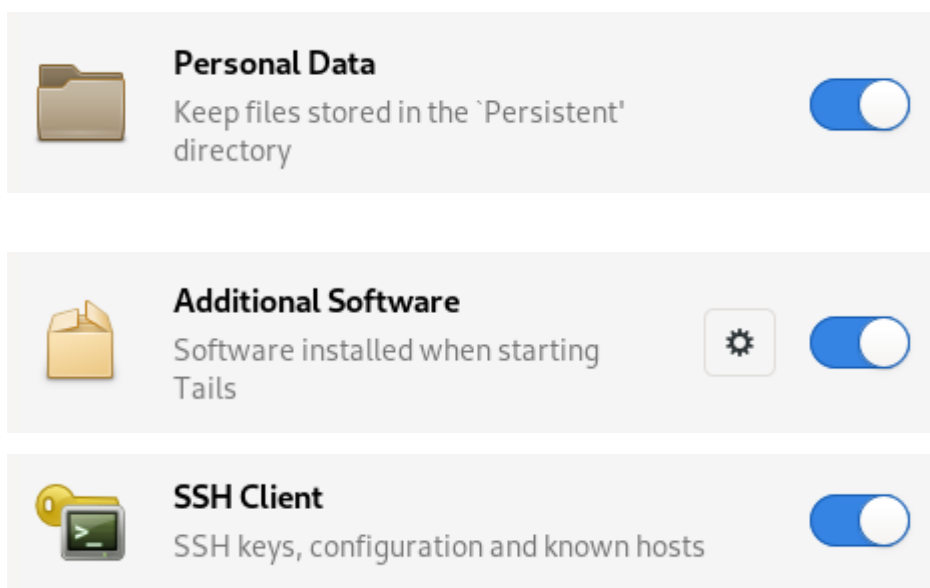
4.0 Preparations prior to use of this addon

To run this script from version 0.52 or higher you need the following things.

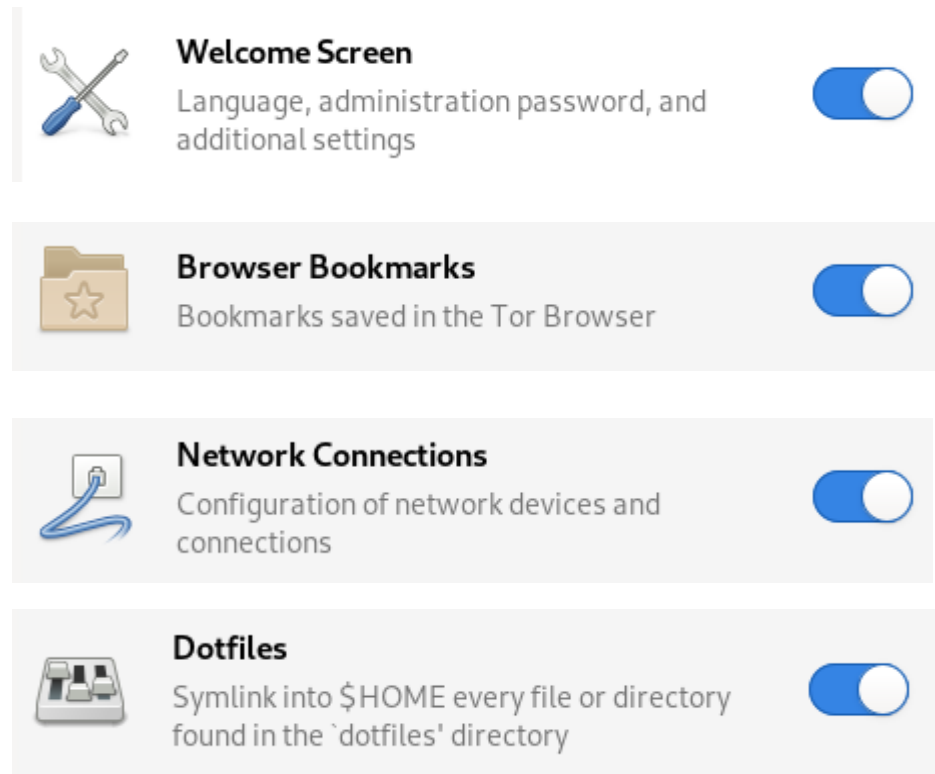
- One USB drive with at least 8 GB capacity.
- A Tails Version 4.14 or higher. Tails have an excellent documentation for the installation process itself.

<https://tails.boum.org/install/index.en.html>

After the successful installation of Tails 4.14 or higher, you need to create a “Persistent Volume”. To run this script you need at least the following 3 options activated inside of the “Persistent Volume”. Without these 3 must have options enabled, the add-on will not work correctly as expected.



The following 4 persistent volume options are not really mandatory for the add-on to run, but I would recommend to use them as well, I would say they are “nice to have optional features”.



The remaining 5 persistent volume options available are :

- Printers
- Thunderbird
- GnuPG
- Bitcoin Client
- Pidgin

If you use them or not, depends on your own personal choice depending on how you use Tails. My add-on can also backup all the files of a persistent volume if you would like to do so. After the creation of the persistent volume, you have to restart Tails to make all the changes active.

At this stage, from now on, please remember to do the following when you start Tails.

- You have to open the persistent volume on every start of Tails if you want to use the add-on. Of course, you can start Tails without the persistent volume activated, but the add-on itself and all the data is stored on this persistent volume aren't usable, even the stored WiFi passwords aren't usable.
- The administration password of Tails also needs to be set on every start of Tails if you don't decide to store your settings of the greeting-screen . If you don't set an administrator password, the add-on won't be able to change the default local firewall. The script changes only one unique little setting inside the firewall of Tails.

The changed setting is

```
sudo -S iptables -I OUTPUT -o lo -p tcp --dport 9999 -j ACCEPT
```

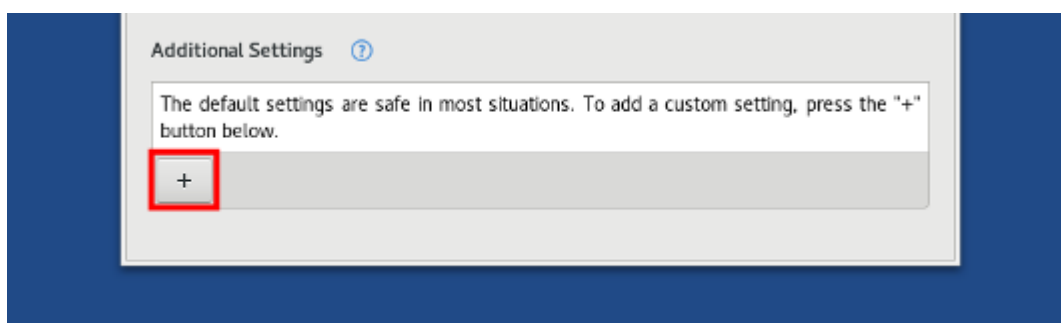
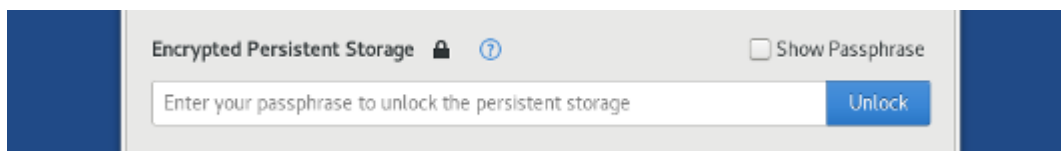
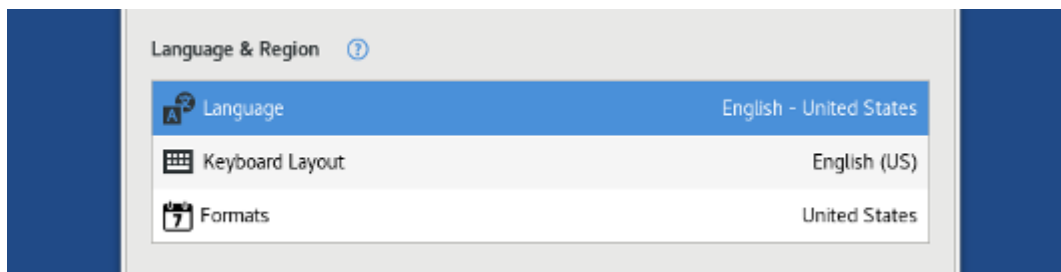
This little change allow us to build a local socks5 proxy over SSH. Without this modification, the predefined default rules from iptables would block any connection attempt made to port 9999 from the loopback device 127.0.0.1

5.0 Installing the add-on

Let us assume now, you created the persistent volume successfully.

If you didn't choose to store the values of greetings screen, you have to fill them up on every startup of Tails.

- Language
- Keyboard Layout
- Formats
- The password for the Persistent Volume
- The administrator password



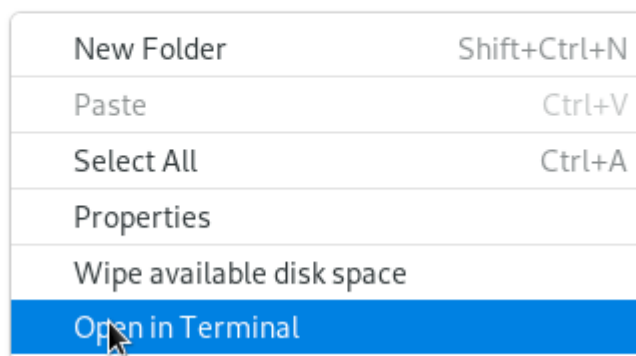
The following shortcut keys (greeting screen) are working on Tails 4.14 or

higher.

Keyboard shortcuts

Alt+L	Language
Alt+K	Keyboard Layout
Alt+F	Formats
Alt+P	Persistent Storage
Alt+A	Additional Settings
Ctrl+Shift+A	Administration Password
Ctrl+Shift+M	MAC Address Spoofing
Ctrl+Shift+N	Network Configuration
Alt+S	Start Tails

After successfully booting Tails, please open a terminal inside of the persistent folder area (right click anywhere inside the area).



After the terminal is opened, please copy this following text into the clipboard of Tails.

git clone <https://github.com/swtor00/swtor-addon-to-tails>

And copy the value of the clipboard with the shortcut <Ctrl><Shift><v> into the already opened terminal. To complete the unfinished command, you have to press [Return].

By now, you have to wait. Depending on the speed of your current Internet connection, after a while you should find a folder called “swtor-addon-to-tails”. Please don’t worry about the connection you made to Github (a Microsoft company since June 2018). You are already using the onion-network of Tails to connecting to the Github Server and the only thing that Github is knowing, is the IP-address of the last “Exit-Node”.

My personal advice for you, the reader of this documentation :

NEVER MAKE A VISIT TO THE GITHUB SITE THAT HOSTS THIS ADD-ON ON A OTHER BROWSER THAN THE TOR-BROWSER OF TAILS !!

Before you do anything inside the directories of the add-on, you should first make a few important decisions about the use of the add-on itself. The configuration of the add-on is written in a single plain text file. It can be edited over the Gnome Editor (gedit) or even vim / nano if you would like to edit the file this way.

Prior to executing anything, the complete path to this configuration file is as follows.

~/Persistent/swtor-addon-to-tails/swtorcfg/swtor.cfg

The default configuration file swtor.cfg for version 0..52, looks like this.

```
SWTOR-VERSION:0.52
TAILS-VERSION:4.14
STATE: BETA
HOMEPAGE: https://github.com/swtor00/swtor-addon-to-tails
JOTV :
```

```
-----
"Fight fire with fire"
-----
```

OPTIONS FOR THE SWTOR-ADDON

```
IMPORT-BOOKMARKS:NO
GUI-LINKS:YES
BROWSER-SOCKS5:YES
CHECK-UPDATE:NO
BACKUP-FIXED-PROFILE:NO
BACKUP-APT-LIST:NO
```

All above entry's showed after “OPTIONS FOR THE SWTOR-ADDON” are configurable options witch can be enabled or disabled for the future use. Please note that all this options are in Capital-letters.

Let us begin with the first option, on the first line.

IMPORT-BOOKMARKS:NO

If you change the predefined value to YES, my personal TOR-Browser bookmarks (with a few fantastic onion sites included) are directly imported on the first startup of the add-on. The default value of this option is NO, for one big reason. I don't like to hear, that someone's large personal bookmarks are accidental overwritten by my script on first startup.

GUI-LINKS:YES

If you change the value to NO you can only start the script over terminal. Most users should use here the default value YES.

BROWSER-SOCKS5:YES

Currently this value should always be YES , In the near coming future it may come with a additional settings like BROWSER-PROXY or RDP-CONNECTION / VNC-CONNECTION.

CHECK-UPDATE:NO

If you would like to look for a automatic installed update on startup of the add-on, please change the value to YES. In the moment you change the value to Yes. If you do so, please not that on every startup of the add-on the the Github Server will be contacted, to check for a newer release.

BACKUP-FIXED-PROFILE:NO

BACKUP-APT-LIST:NO

Please don't change none of the 2 above options to YES. If you would do against my advice, a backup of the persistent volume would need very much space to operate correctly. If you leave the above values at the default state NO, the created backup of the Persistence volume will have a size somewhere between 3 - 5 MB.

6.0 Configuring the required SSH-connection for the add-on

For this final configuration step, we need a valid SSH account from anywhere on the Internet or at our home-server. You may even try first to test this new SSH connection with another operating system like Windows, Linux or even an Apple system which contains all the software needed to establish a SSH connection, generally all modern operating system ... (including Microsoft Windows10 Version 1803 or higher) do have this SSH-software included.

In my humble opinion, DO NOT even think about using this. Under all circumstances, it's an insanely bad idea to use this SSH-connection anywhere outside of the Tails-system !!

If you really want to use a socks5 SSH connection to hide your browser traffic with any other operating system than Tails, you should create a complete new login on a remote SSH-host only for that purpose ! If you use these same SSH-credentials outside of Tails, you would leak your current WAN IP-Address to the owner and other users of the remote SSH-host immediately the moment you try to connect over SSH without the protection of the Onion-Network in the background over 3 nodes. A simple command "who | more " inside a Linux terminal would list all current connected users and the corresponding IP-Address from the location a user is connected . An simple example of the command could look this.

eao	pts/7	2018-xx-23 17:27 (81.221.101.10)
dyama	pts/8	2018-xx-25 02:07 (158.3.77.185)
tt0077	pts/9	2018-xx-25 20:08 (51.41.129.24)
jose1711	pts/11	2018-xx-08 09:14 (186.177.234.117:S.0)
piny	pts/13	2018-xx-27 07:48 (213.41.33.159)

In the perfect case that we are using the Onion-Network inside Tails, the printed IP-Address would be only be from our currently used Exit Node 3. If we wouldn't use the onion-network at all, the printed IP-Address would be our currently used WAN IP from the ISP. Therefore never use this ssh login outside of tails !

An normal SSH account normally consists of the following 3 needed information for a successful connection.

- A username including a valid corresponding password for that used user, that will be transmitted on first connection.
- A destination port. The default port for a SSH communication is TCP port 22.
- A DNS Name like “mugo.redpill.moo” or a simple IP V4 IP-Address like “46.88.199.206”

All the configuration files for an SSH connection reside inside the directory /home/amnesia/.ssh. If this directory is empty, it means that we have never contacted any SSH-server before with our current Tails system.

To test our connection and see if we can successfully login over SSH, we need to open a terminal and execute the following command. (You can replace the values in this example with the values provided by your own SSH-provider.)

```
ssh -p 22 digit1@10.0.1.66
```

Description of the above command in detail :

ssh	The command to communicate encrypted with the other host.
-p 22	22 is the default port for a SSH connection. Due to the behavior of SSH , it isn't always necessary to add -p 22 for every connection. If your SSH-providers doesn't use the default port 22, then the -p option should be used every time with the correct port number.
digit1	The username of the SSH login
10.0.1.66	The IP-Address of the remote server. We could also provide a DNS Name instead of a IP-Address.

In the case of the following scenario where we have never made an SSH connection with our new Tails Medium to an SSH-server with the IP-Address 10.0.1.66, we will see a warning like following one.

**The authenticity of host '10.0.1.66 (10.0.1.66)' can't be established. RSA key fingerprint is 90:8c:7d:f8:ae:1a:09:60:44:08:3b:d9:c9:f7:c4:76.
Are you sure you want to continue connecting (yes/no)?**

This is the so called “public fingerprint” of the SSH-Server we are trying to connect to. The moment we type “yes” inside the terminal, the public fingerprint for this specific server with the IP 10.0.1.66 is then stored inside the file `~/ssh/known_hosts`.

After storing this public key inside Tails, on every connection we make to 10.0.1.66, the already stored value inside the file `/ssh/known_hosts` will be compared against the value that the server provides upon connecting. If there is a match of both values, we can continue to establish our connection. If the two values don't match, then there is something wrong ! If you find the following entries inside your log file or the terminal, be very carefully with your next action.

WARNING : REMOTE HOST IDENTIFICATION HAS CHANGED. IT IS POSSIBLE THAT SOMEONE IS DOING SOMETHING NASTY !

- It may be that someone is trying to make you think that you are connecting to the host 10.0.1.66 ,but you aren't, this is called a “man in the middle attack”.

https://en.wikipedia.org/wiki/Man-in-the-middle_attack

Someone could now steal your current password for that particular SSH-host or even worst, steal your current public SSH key if you ignore this warning and connect to this possible evil or nasty SSH-Server !!!!

- Or that the public key of the server has been replaced for some reason, possibly the remote server SSH-Server was replaced due to a hardware failure.

Next, you should see the password login, for the requested user login on the remote server. You can now type the password for that account and the remote shell should appear straight afterwards. To leave the remote session to the SSH-Server please type “exit” and press [Enter]. As a replacement you could also use the keyboard shortcut <ctrl><d> to close the session.

Provided we can login to the remote server without any error, our next step would be to make this SSH login password free in the future. Of course you could also customize a few things like changing the current password or a few other things also. If you change the current password, please write it down somewhere and store it in a safe place. If you have to start with a new empty Tails (Clean Tails Clone) , you may need the change password, to transfer the backups you made.

Our next terminal command is used to create the private / public key pair for all future SSH-communication inside of Tails. The command to accomplish this, is the following one. Please be sure to execute this command on the local Tails system Terminal and not in a SSH session over the Terminal.

```
ssh-keygen -t rsa -b 4096
```

After a short initialization time to generate the public and private keys, we have the keys created. This is now our own personal “holy-grail” of encrypted communication for use inside of Tails and should be saved on a regular basis. Inside of the script you could make backup of this keys and restore them on new created Tails medium, if you need this.

Now we can copy our previous created public key to our SSH-server. There is a special SSH command to do this.

```
ssh-copy-id -p 22 -i ~/.ssh/id_rsa.pub digit1@10.0.1.66
```

- Please replace 22 with the correct port-number you would like to use
- Please replace digit1 with your own username
- Please replace 10.0.1.66 with your own IP-Address or DNS-Name

Some older Unix systems don't support the ssh-copy-id program, so with a few little bash-tricks it's also possible to transfer the public key to the foreign SSH-server with the standard Unix commands every system should clearly understand.

```
cat ~/.ssh/*.pub | ssh -p 22 digit1@10.0.1.66 'umask 077; \  
cat >>.ssh/authorized_keys'
```

By now it should be possible, to make an SSH connection with Tails to the remote SSH-system 10.0.1.66 without any password or any other additional typing with the keyboard. Please test it that it works, like expected ...

- For every ssh-host you would like to connect to, you have to execute the command `ssh-copy-id` once or you have to type the password again on every connection you make !
- You should test every additional ssh-connection carefully so that there is no confirmation needed like adding the public key to the `known_hosts` file inside the directory `~/.ssh`.

As soon as you have at least one SSH connection that works properly, you can create the configuration file that is needed by the add-on. Inside the “doc” directory of the add-on , you will find a small example pdf (sample-configuration.pdf) that explains exactly how to create this configuration file. The configuration of all possible SSH connections that this add-on can use are defined in this single file.

`~/Persistent/swtor-addon-to-tails/swtorcfg/swtorssh.cfg`

SSH itself is a very complex piece of software, if you would like to have more information about SSH in general or you need some cool advanced troubleshooting tips, you should have a closer look using the TOR-Browser to navigate to the following url.

<https://www.allitebooks.in/ssh-secure-shell-2nd-edition/>

<https://www.openssh.com/manual.html>

Tips for troubleshooting :

All SSH-connections made with the swtor add-on have a “verbose” output on all actions. You find all the logs inside the following directory.

`~/Persistent/swtor-addon-to-tails/swtorcfg/log`

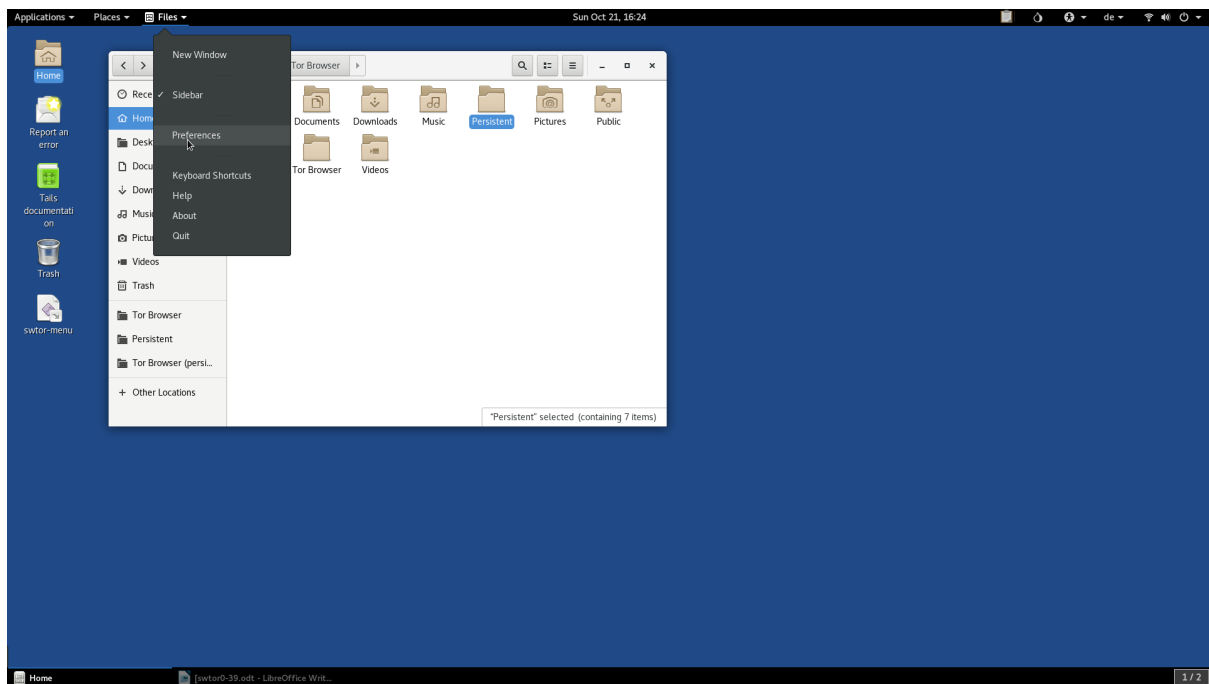
7.0 Executing the add-on the first time

The default behavior of the Tails-System doesn't allow the execution of shell-scripts over the GUI Interface. If you don't want to execute the scripts over the GUI of Tails, you must execute the shell-scripts with a terminal. In this particular case you can skip the configuration of the GUI to execute shell-scripts and write directly `./swtor.-setup.sh` to start the script.

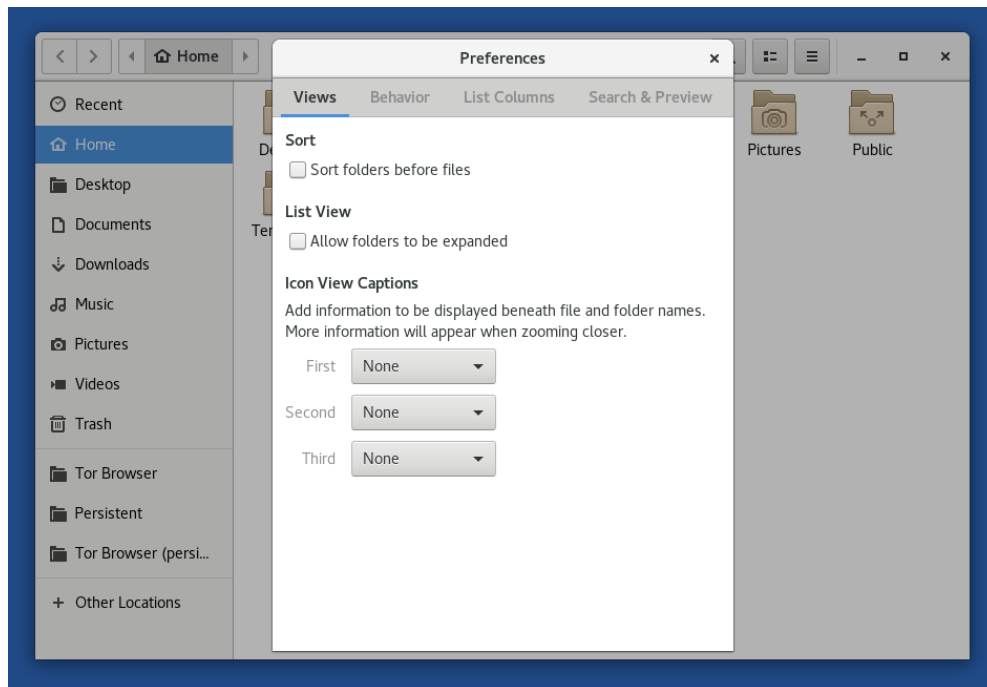
```
cd ~/Persistent/swtor-addon-to-tails/scripts  
./swtor-setup.sh
```

Please make the following little changes inside Tails to make all shell scripts generally executable. You have to repeat this step, on every startup of tails !

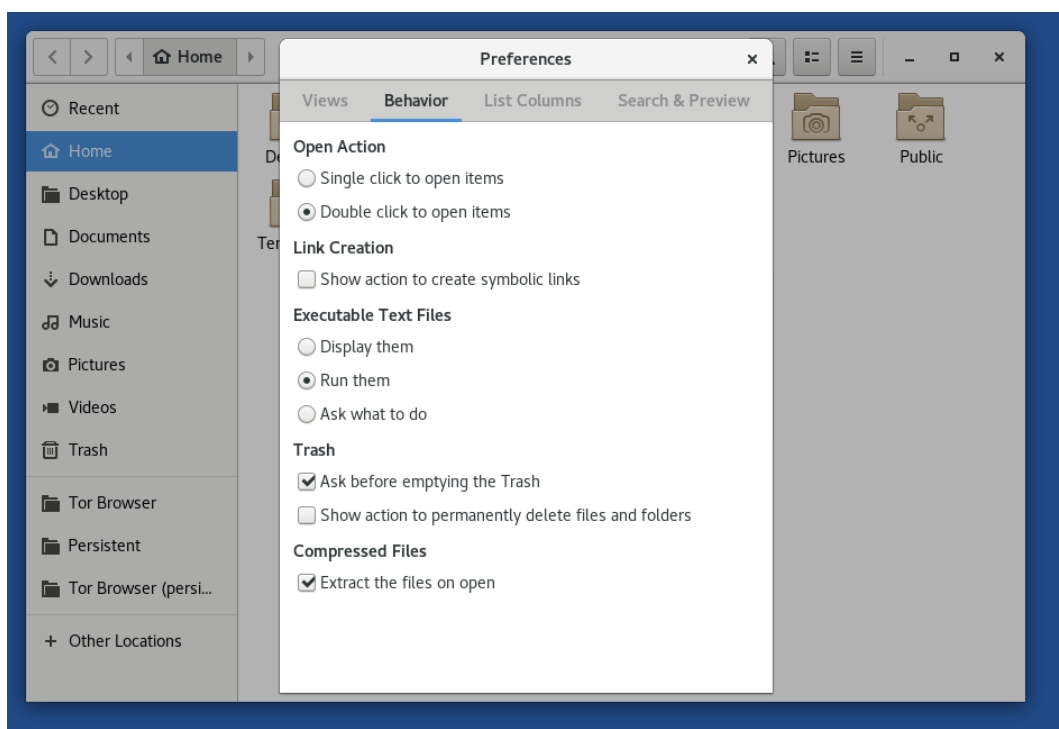
- 1.) Open “Home” on the tails desktop
- 2.) Open “Files” and “Preferences”



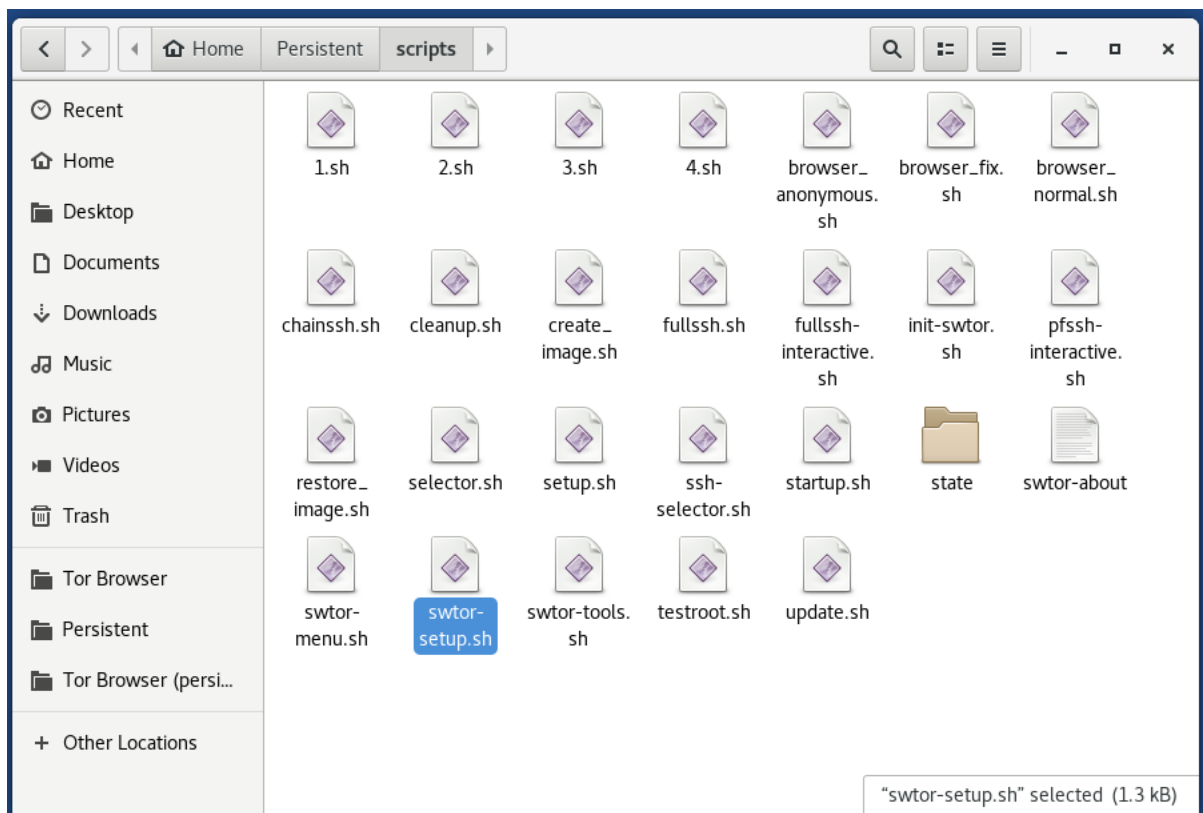
3.) Open the “Behavior” Tab



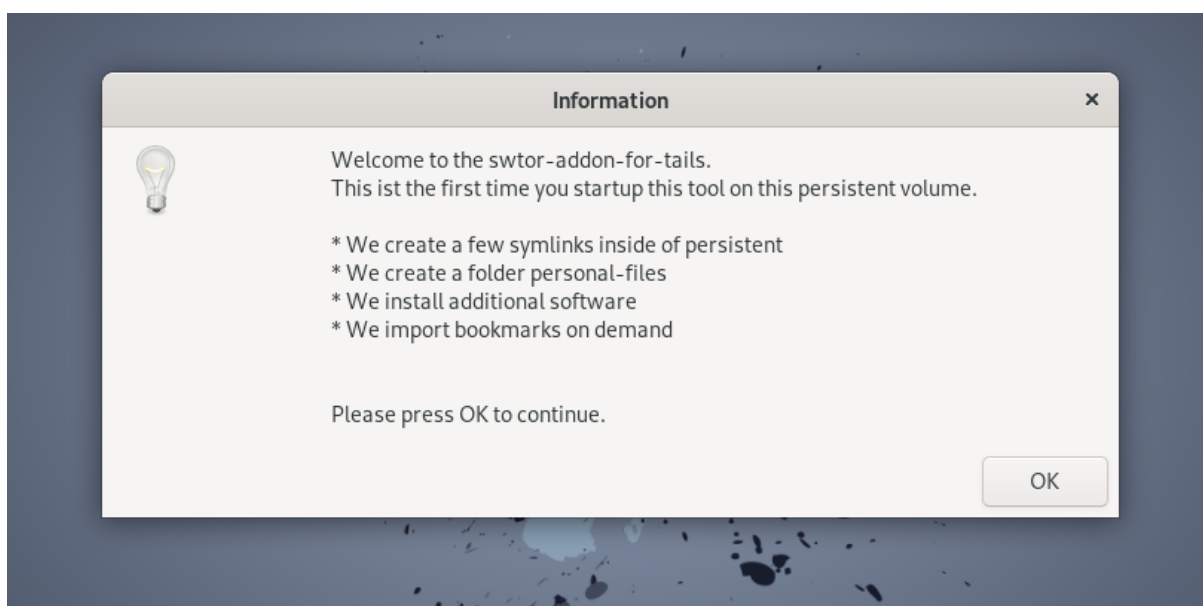
4.0 Activate the option “Run them”



Next, navigate to the folder `~/Persistent/swtor-addon-to-tails/scripts`



Please execute first the file “swtor-setup.sh” with a right mouse double click → execute or do a double-click on it. Within a few seconds, you should see the first window pop up.



After pressing the OK Button, the following 4 symbolic links inside of the root folder of Persistence Volume are created during this first startup

~/Persistent/scripts

/home/amnesia/Persistent/swtor-addon-to-tails/scripts

~/Persistent/settings

/home/amnesia/Persistent/swtor-addon-to-tails/settings

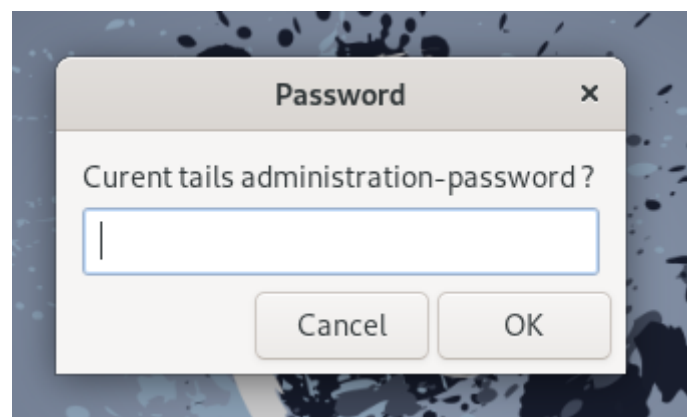
~/Persistent/swtorcfg

/home/amnesia/Persistent/swtor-addon-to-tails/swtorcfg

~/Persistent/doc

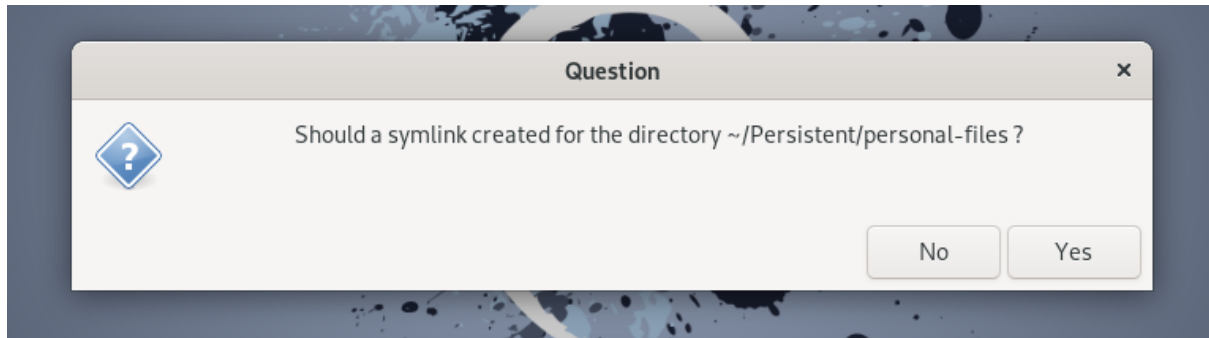
/home/amnesia/Persistent/swtor-addon-to-tails/doc

In the next dialog you have to type the password for the tails administration .



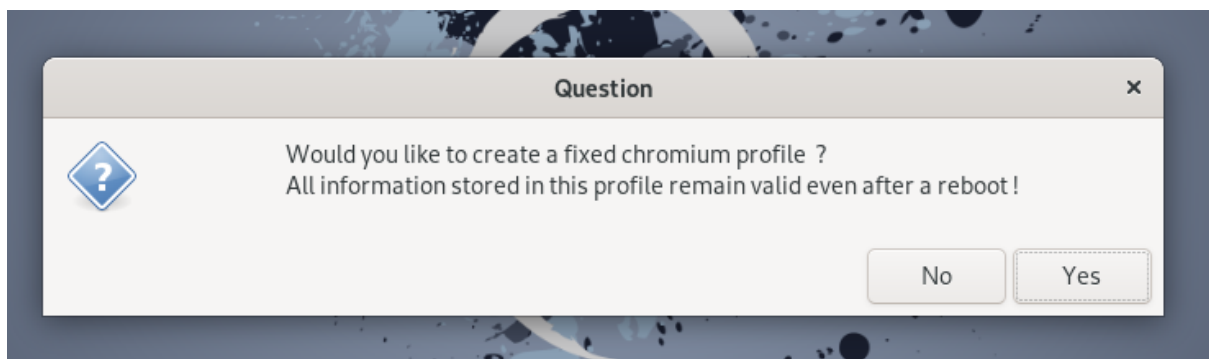
In the case, that the provided password was correct, the script does continue. Otherwise the script does abort and has to be started again.

The next dialog would come up ...



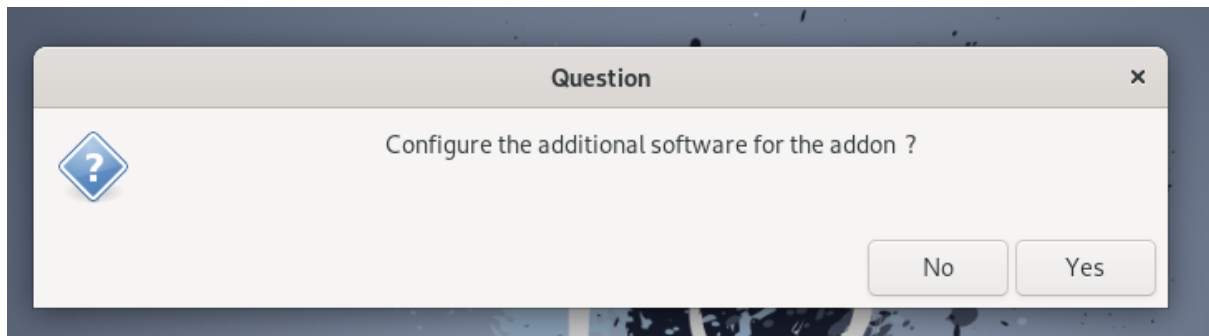
If you answer “YES” it will ask for symbolic link name, otherwise no symlink to the directory is created.

The next dialog would come up ...



Most users can answer “YES” here. If you answer NO, you can only choose between 2 chromium profile.

The next dialog would come up ...



Please only say “NO” if you already installed the following software on you currently used Tails.

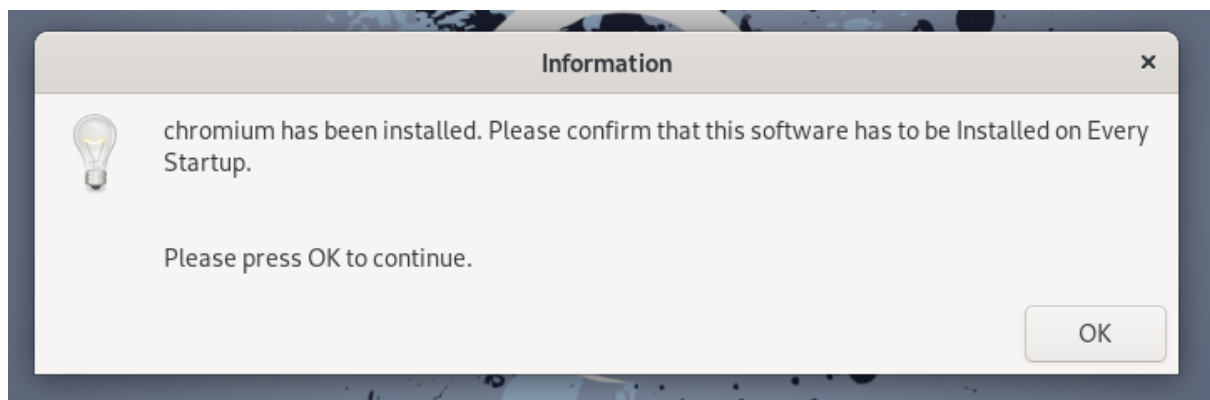
- chromium
- chromium-sandbox
- html2text
- sshpass
- yad

If you press “YES” the above listed software will be installed.

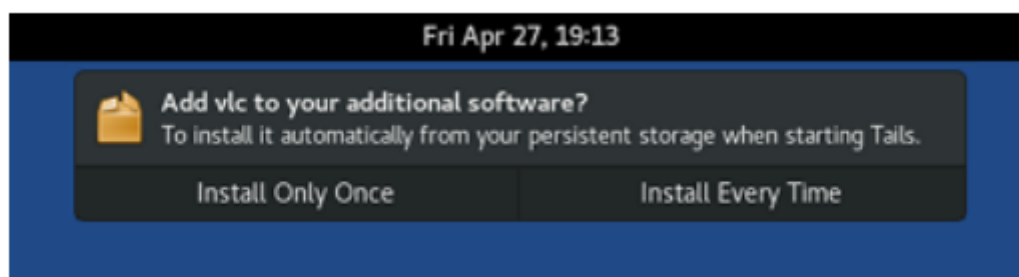
Warning :

This initial step to install the additional software may run a very long time. Please don't interrupt the script during this installation and wait until it is confirmed that the software is installed successfully.

You should see a confirmation window for every software installed (like chromium in this window) and the 4 others as well.

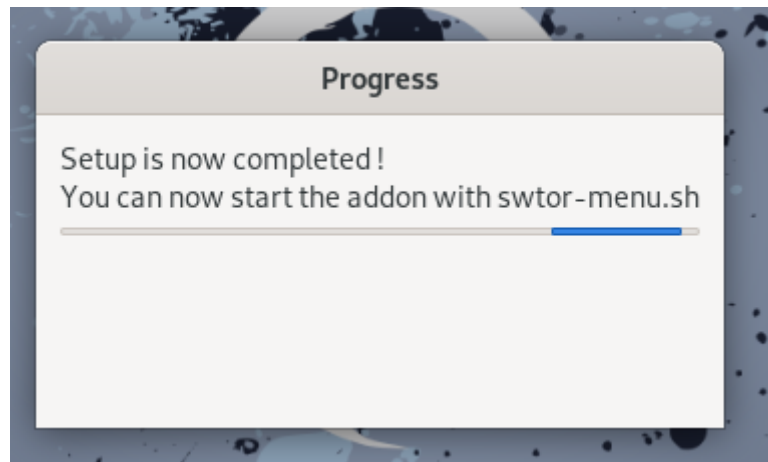


A few seconds later ,after you see this information window for every software, you should see a little Tails notification on top of the screen as well.



Please press for all the 5 installed software packages the Button "Install Every Time"

End here we are ... at the end of the initial setup-routine.



8.0 Use of the add-on, after the execution of setup-routine